REMARKS

Claims 10-20 are pending in the Application. All of the claims have been rejected. In view of the following remarks, Applicant respectfully requests reconsideration of the Application.

Rejections Under 35 USC §102(b)

On page 2 of the Office Action, the Examiner rejected claims 10-21 under 35 USC §102(b) as being anticipated by Misra (USPN 5,757,920, hereinafter *Misra*). Applicant traverses.

Misra does not prevent further access to a first server

Independent claims 10, 18, and 21 recite in part "receiving a current access request to access a secured item via a second server machine of the plurality of server machines" and "reconfiguring the first server machine to ***prevent further access*** by the user to secured items via the first server machine." In order to "prevent further access" the user or machine must currently have access, which is subsequently prevented.

Misra does not provide any support for subsequently preventing access once the user or machine is allowed to access a domain. *Misra* only discusses systems and methods allowing the initial authorization to access the information in the domain. Specifically, *Misra* provides a system whereby the distributed system is logically partitioned into domains. Each domain implements its own administrative and security policies, whereby each domain controller serves as a centralized location for storing knowledge about the namespace of the distributed system (col. 4, ln 31-37 and ln 46-52). Each domain controller holds information about users and machines for which the domain is the home domain.

Furthermore, logon certificates, which are secured packages holding credentials information sufficient to establish the identity, rights, and privileges of a user/machine,

are stored on a portable storage medium or in memory of the portable computer (Abstract; col. 1, ln 60-65). Logon certificates provide a way to "demonstrate that the user/machine has sufficient credentials to connect to the non-home domain without contacting the home domain (col. 5, ln 14-16).

Thus, Misra only teaches systems and methods for initially accessing a domain, but does not provide any teaching or suggestion for preventing further access once access has been granted.

Misra does not reconfigure servers

Misra does not teach or suggest a reconfiguration of servers. *Misra* only discloses different authentication methodologies (e.g., home-domain authentication versus a logon certificate). Specfically, the portions of *Misra* cited for support regarding the reconfiguration of the first and second server machines do not discuss a "reconfiguration." Instead, one section only discusses the use of a domain control to authenticate a user/machine for a home domain, while using logon certificates to allow the user/machine to connect to a non-home domain (col. 5, ln 10-21). This does not provide any support for reconfiguring a second server machine to permit access by the user.

Similarly, the second cited section refers to the use of session keys and secret keys in a Kerberos protocol associated with the logon certificate (col. 7, ln 53-65). Applicant does not see how session keys and secret keys reconfigure the first server machine to prevent further access by the user.

Misra does not reconfigure based on the request for access at a second server

Furthermore, the limitation of "***subsequently receiving*** a current access request to access a secured item via a second server machine of the plurality of server machines" and "reconfiguring the first server machine to prevent further access by the user to

secured items via the first server machine" are interconnected. That is the first server machine is reconfigured to prevent further access based upon the request to access the secured item via the second server machine. In exemplary embodiments, one location (i.e., the first server machine) is no longer responsible for the user, while the second location (i.e., the second server machine) takes over responsibility for the user (see *Application* [0123]). In these embodiments, the user only accesses the secured items from a single location at any one time.

In contrast, there is no mechanism in *Misra* to manage the local servers in a centralized manner whereby a first server can be reconfigured to prevent access to the user or machine, while a second server is reconfigured to allow access to the user or machine. Instead, each domain controls its own access and security independent of the other domains. In fact, a user in *Misra* could, conceivably, access information from multiple domains at the same time.

While the Examiner cites portions of *Misra* for support for the reconfiguration of the first and second server machines, the cited portions are distinct from each other. In other words, there is no relationship between the two cited portions whereby access to one server or domain triggers non-access to the other server or domain in *Misra*.

For at least these reasons, *Misra* does not anticipate independent claims 10, 18, and 21. Additionally, because claims 11-17 and 19-20 depend from claims 10 and 18, respectively, these claims are not anticipated for at least the same reasons.

CONCLUSION

Based on the foregoing remarks, Applicants believe that the rejections in the Office Action of February 10, 2006 are fully overcome, and that the Application is in condition for allowance. Should the Examiner have questions regarding the case, the Examiner is invited to contact Applicant's undersigned representative at the number given below.

Respectfully submitted,

Hal Hildebrand et al.

Date: 8/10/06 By: Susan Yee

Susan Yee, Reg. No. 41,388
Carr & Ferrell *LLP*
2200 Geng Road
Palo Alto, CA 94303
TEL: (650) 812-3400
FAX: (650) 812-3444